Online Safety Policy

Policy

Amberley Parochial School

Providing the rich soil that enables
our children to develop deep roots and flourish.

Chair of Governor: Dr Holmes
Approved by: FGB Committee
Approved on: Spring Term Two 2020
Review Date: Spring Term Two 2021
Other relevant policies: Safeguarding Policy, Special Educational Needs and Disabilities and

This policy should be read in conjunction with Annex C of KCSiE 2020 on remote learning.

Scope of the Policy

This policy applies to all members of the Amberley Parochial School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online safety lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing Co-ordinator and Edit support services.
- The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).
- The Head teacher /Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Senior Leadership Team will receive regular monitoring reports from the Online safety lead.

Online safety Coordinator:

At Amberley Parochial Primary School, the Online safety lead role will be part of the Designated Safeguarding Lead role,

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff (Edit)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found later in this document).
- meets regularly with online safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governors meetings
- reports regularly to Senior Leadership Team

Technical staff (Edit):

The Technical Staff for Computing are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority ~~/other relevant body E-safety Policy /~~ Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy~~, in which passwords are regularly changed~~
- the filtering policy ~~(if it has one),~~ is applied and updated on a regular basis as advised by SWGfl and that its implementation is not the sole responsibility of any single person ~~(see appendix "Technical Security Policy Template" for good practice)~~
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email will be~~is~~ regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher/online safety lead / Governor for investigation / action / sanction
- that monitoring software / systems will be~~are~~ implemented and updated as agreed in school policies. Monitoring software is constantly evolving so the process is always under review.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP)
- they report any suspected misuse or problem to the Head Teacher/ online safety lead for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Acceptable Use policy Agreements
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

(N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.)

Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy Agreements
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign the Staff/ Guest/ Volunteer ~~Community~~ User AUP Agreement before being provided with access to school systems. ~~(A Community Users Acceptable Use Agreement Template can be found in the appendices.)~~

Policy Statements

Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. *(N.B. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.)*
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (Edit) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to ~~the~~ relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers ~~(see appendix for further links / resources)~~*

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision when requested

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online safety lead will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / TA meetings / INSET days.

- The Online safety lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the school to ensure that the managed service provider (EDIT) carries out all the online safety measures that would otherwise be the responsibility of the school, as detailed below. It is also important that the managed service provider is fully aware of the school Online Safety Policy / Acceptable Use Agreement Policies. The school should also check their Local Authority ~~/ Academy~~ Group / other relevant body policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities

~~A more detailed Technical Security Template Policy can be found in the appendix.~~

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority Group / other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All pupils will initially use class usernames. Pupils ~~(~~at KS2 and above~~)~~ may eventually be provided with a username and secure password by the Computing lead who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.~~)~~
- The “administrator” passwords for the school ICT system, used by the Network Manager ~~(~~and Online safety Governor~~, Cliff Hodgson)~~ must also be available to the Head teacher and kept in a secure place (eg school safe)
- The managed service provider (Edit) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate

Formatted: Font: Not Bold, Not Highlight

Formatted: Not Highlight

Formatted: Font: Not Italic, Not Highlight

Formatted: Not Highlight

licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the school will assess ~~need to decide on~~ the merits of external / internal provision of the filtering service ~~– see appendix~~). There is a clear process in place to deal with requests for filtering changes. Staff are provided with the capability for bypassing the filter system, in order to access relevant sites for educational purposes. They will remain vigilant when using this access and will ensure that passwords remain secure. ~~(see appendix for more details)~~
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- The school has provided enhanced filtering allowing ~~/ differentiated user-level filtering (allowing~~ different filtering levels for ~~different ages / stages and~~ different groups of users – staff / pupils ~~/ students~~ etc)
- School technical staff (Edit) are investigating SWGfl tools to ~~regularly~~ monitor and record the activity of users on the school technical systems. ~~and U~~users are made aware of this in the Acceptable Use Agreement Policies. ~~*An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agre*~~
- Appropriate security measures are in place ~~(schools may wish to provide more detail)~~ to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure ~~policy~~ is in place ~~(to be described)~~ for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. Visitors are only allowed access to the wifi service.
- At the present time, pupils are not permitted to use school devices out of school unless directly supervised by a member of staff. A more liberal policy for out of school use of school devices for pupils will be agreed when the requirement is more certain. ~~An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of scho~~
- Restrictions are ~~An agreed policy is~~ in place ~~(to be described) that allows staff to / forbids~~prevent staff from ~~downloading executable files and~~ installing programmes on the school server. ~~school devices.~~
- ~~An agreed policy is in place (to be described) regarding the use of r~~Removable media (eg memory sticks / CDs / DVDs) may be used by staff on school PCs and laptops. ~~by users on school devices.~~ Personal data ~~cannot be~~ sent over the internet or taken off the school site should be ~~unless~~ safely encrypted or otherwise secured. ~~(see School Personal Data Policy Template in the appendix for further detail)~~ The school is investigating software that will enforce this.

Formatted: English (United States), Not Highlight

Formatted: English (United States), Not Highlight
Formatted: Font: Not Italic, English (United States), Not Highlight
Formatted: Font: Not Italic, English (United States), Not Highlight
Formatted: Font: Not Italic, English (United States), Not Highlight
Formatted: Not Highlight
Formatted: Font: 11 pt, Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Font: Not Italic, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Not Highlight
Formatted: Font: 11 pt, Not Italic, Font color: Auto, Not Highlight
Formatted: Font: 11 pt, Not Bold, Not Italic, Font color: Auto, Not Highlight

Mobile Technologies ~~(including BYOD/BYOT)~~

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies element of this policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy Agreements, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online safety education programme.

- **The school allows:**

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**		**Student owned**	**Staff owned (must be authorised**	**Visitor owned**
Allowed in school	*Yes*	*Yes*		*No*	*Yes*	*Yes*
Access to school services (password controlled)~~Full network access~~	*Yes*	*No~~Yes~~*		*No*	*Yes*	*No*
Filtered access to wifi	Yes	Yes		No	Yes	Yes
Unfiltered access to wifi	Yes	No		No	Yes	Yes (on request)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and ~~students /~~ pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of ~~students /~~ pupils are published on the school website / social media / local press. ~~(may be covered as part of the AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix)~~
- In accordance with guidance from the Information Commissioner's Office, Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is~~n~~ not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published ~~/~~or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other ~~students /~~ pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow schoo~~/ *academy*~~ policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes without prior permission from the Head Teacher.
- Care should be taken when taking digital / video images that ~~students /~~ pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- ~~Students / p~~Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include ~~students /~~ pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- ~~Students' /~~ Pupils' full names will not be used anywhere on the school~~a~~ website ~~or blog,~~ particularly in association with photographs.
- ~~Student's /~~ Pupil's work can only be published with the permission of the ~~student /~~ pupil and parents or carers.
- Images taken on school cameras (and similar devices) will be removed from the device as soon as is possible and practical.

Formatted: Font: 11 pt, Font color: Auto

Formatted: Font: 11 pt, Font color: Auto

Formatted: Font: 11 pt, Italic, Font color: Auto

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- **It has a Data Protection Policy.**
- **It has paid the appropriate fee to the Information Commissioner's Office (ICO).**
- **It has appointed a Data Protection Officer (DPO).**
- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.**
- **The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.**
- **Where special category data is processed, a lawful basis and a separate condition for processing have been identified.**
- **Data Protection Impact Assessments (DPIA) are carried out.**
- **It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.**
- **Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.**
- **There are clear and understood data retention policies and routines for the deletion and disposal of data.**
- **There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.**
- **Consideration has been given to the protection of personal data when accessed using any remote access solutions.**
- **All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **All staff receive data handling awareness / data protection training and are made aware of their responsibilities.**

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- **The data must be encrypted and password protected.**
- **The device must be password protected.**
- **The device must offer approved virus and malware checking software.**

- **The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.**

Communications

~~A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:~~

When using communication technologies Amberley Parochial Primary School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online safety discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

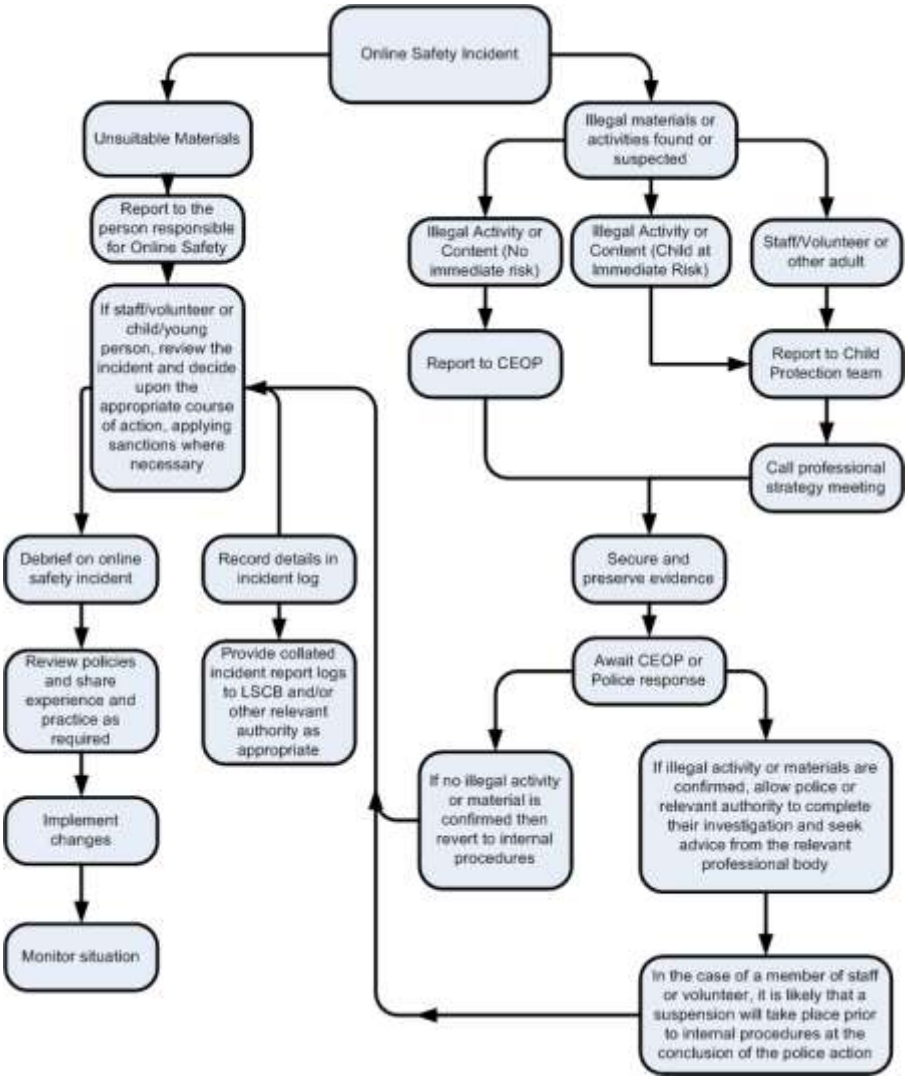
- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school
- The school Governing Body will decide if and how to respond to incidents of social media comments about the school.~~should effectively respond to social media comments made by others according to a defined policy or process~~

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online safety services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, and~~who~~ understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The incident record ~~completed form~~ should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Acceptable Use Agreements are now completed online using Microsoft forms.

Staff / Volunteer / Guest Acceptable Use Policy

1.For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, website etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- Yes
- No

2. I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. I will not download these images to personal devices. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. Any email sent to pupils will be done so using official school email addresses.
- I will not invite children and young people (past or present) onto personal social networking sites.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

- Yes
- No

3. The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up and will use encrypted or password protected memory sticks if transporting data.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Yes

No

4.When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Yes

No

5.I understand that when delivering remote education online, the same principles set out in the school staff code of conduct policy will apply.

Yes

No

6. I am aware of the dedicated collection of resources (Annex D) to support safe remote education, virtual lessons, and live streaming, and the resources set out to signpost parents and carers to help them keep their children safe online (which are also detailed on the school website).

Yes

No

7. I am aware that schools can access the free Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. (Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.)

- Yes
- No

8. I am aware that all school staff should continue to act immediately (following the child protection policy and the processes set out in Part 1 of Keeping Children Safe in Education) if they have any concerns about a child or young person's welfare, whether the child or young person is physically in school or learning from home.

- Yes
- No

9. **When working remotely, I am aware that I will need to adhere to the following GDPR considerations when managing personal data:**

- taking care not to share contact details when emailing multiple people
- being careful when sharing usernames and other personal data for access to online resources
- providing access to school data systems safely
- providing or making available sufficient information to data subjects, pupils, student, parents and carers to raise awareness about the personal data captured during lesson recordings, particularly where cameras are switched on

Yes

No

10. **I understand that I am responsible for my actions in and out of school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Yes

No

11. I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Please enter your name in the box below:

12.Date:

becoming reflective, independent and aspirational learners for life

Amberley Parochial Primary School

Pupil Acceptable Use Policy Agreement: EYFS

I choose to stay safe

- I will tell an adult straight away if I see anything scary or anything that makes me feel uncomfortable online and I will not show it to other children.

I choose to be kind and helpful

- I will only use polite words when using the computers.

I choose to be honest

- I will only use the school's computers, iPads or tablets for things a teacher has asked me to do.

I choose to look after property

- I will be careful with computing equipment.
- I will tell an adult straight away if I notice computing equipment is broken or not working.

I understand that:

- If I do not do these things, I may not be allowed to use computers, laptops, tablets or other computing equipment for a period of time.






Child's Name

Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature

becoming reflective, independent and aspirational learners for life

Pupil Acceptable Use Policy Agreement: Key Stage 1

I choose to stay safe

- I know what my personal information is and I will not share it online. ☐
- I will tell an adult straight away if I see anything scary or anything that makes me feel uncomfortable online and I will not show it to other children. ☐
- If anyone online asks me to meet them in real life, I will tell an adult such as my teachers or parents straight away. ☐
- I will never arrange to meet anyone in person after I have met them online. ☐

I choose to be kind and helpful ☐

- I will only use polite language when using the computers and I will not write anything that might upset someone or give the school a bad name. ☐

I choose to be honest

- I will never use other people's usernames and passwords on computers left logged in by them. ☐
- I will only use the school's computer systems for things a teacher has given me permission to do. ☐
- I will not copy, remove or change any other person's files, without their knowledge and permission.

I choose to look after property

- I will be careful with computing equipment. ☐
- I will tell an adult straight away if I notice computing equipment is damaged. ☐

I understand that:

- I know that pictures on the internet can belong to the person who put them there. ☐
- I know that some things on the internet are not true. ☐
- For my own and others' safety and the safety of the school's computer systems, the school will monitor my use of the computer systems, email and other digital communications. ☐
- The school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). ☐
- If I choose not to keep to this agreement I may not be allowed to use computers, laptops, tablets or other equipment until the school feels it is safe and right for me to do so. ☐

Child's Name | Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online. Parent's Signature

becoming reflective, independent and aspirational learners for life

Pupil Acceptable Use Policy Agreement

I choose to stay safe

- I will not disclose or share personal information about myself or others when online. ☐
- If I find something that I think I should not be able to see, I will turn off the screen or close the lid on a laptop or cover on a tablet. I will tell an adult straight away and **not show it to other children**. ☐
- I will tell an adult straight away if I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable online and **not show it to other children**. ☐
- I will not access or share any materials which are inappropriate or may cause harm or distress to others. If I accidentally do so, I will tell an adult straight away and **not show it to other children**. ☐
- If anyone online asks me to meet them in real life, I will tell an adult such as my teachers or parents straight away. ☐
- I will never arrange to meet anyone in person after I have met them online. ☐

I choose to be kind and helpful ☐

- I will only use polite language when using the computers and I will not write anything that might upset someone or give the school a bad name. ☐

I choose to be honest

- I will never use other people's usernames and passwords on computers left logged in by them. ☐
- I will only use the school's ICT systems for things a teacher has given me permission to do. ☐
- I will not download anything without permission. ☐
- I will not bring my own devices (mobile phones / USB devices etc) to school unless I have been given special permission by my teacher. ☐
- I will respect others' work and property and will not access, copy, remove or change any other user's files, without their knowledge and permission. ☐

I choose to look after property

- I will immediately report any damage or faults involving equipment or software, however this may have happened. ☐
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes. ☐
- I will not install or attempt to install programmes, or store programmes on a school computer, nor will I try to alter computer settings. ☐
- I will not attempt to use the school's ICT systems for file-sharing. ☐

I understand that:

- I will acknowledge sources of information and images copied from the internet using a reference. ☐
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may be incorrect and may even be a deliberate attempt to mislead me. ☐
- For my own and others' safety and the safety of the school's ICT systems, the school will monitor my use of the ICT systems, email and other digital communications. ☐
- The school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). ☐
- If I choose not to keep to this agreement I may not be allowed to use computers, laptops or other equipment until the school feels it is safe and right for me to do so. ☐

Child's Name _____ Signed _____

Date _____ I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature _____